# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **05-316102**
(43)Date of publication of application : **26.11.1993**

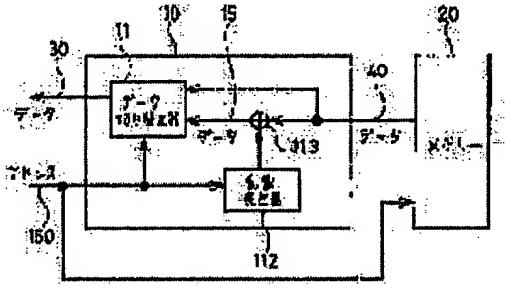
(51)Int.Cl. **H04L 9/00**
**H04L 9/10**
**H04L 9/12**
**H03M 7/00**

(21)Application number : **04-148328**
(22)Date of filing : **13.05.1992**

(71)Applicant : **MEGA CHIPS:KK**
(72)Inventor : **TSUCHIYA TAKASHI**

## (54) DECODER

(57)Abstract:
PURPOSE: To obtain the decoder decoding ciphered data in which data access speed and ciphering performance are satisfactorily compatibile.
CONSTITUTION: Data are read from a memory 20 in which ciphered data and not ciphered data are in existence in mixture, the not-ciphered data or decoding data 15 of the ciphered data are selected depending on an address of the data and outputted externally by a data changeover switch 11, then decoding of data is made difficult because the ciphered data and the not-ciphered data are in existence in mixture in the memory 20, and the not-ciphered data are accessed at a high speed.




LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

**特開平5－316102**

(43)公開日　平成５年(1993)11月26日

| (51)Int.Cl.[5] | | 識別記号 | 庁内整理番号 | ＦＩ | 技術表示箇所 |
|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/00 | | | | |
| | 9/10 | | | | |
| | 9/12 | | | | |
| Ｈ０３Ｍ | 7/00 | | 8522－5Ｊ | | |
| | | | 7117－5Ｋ | Ｈ０４Ｌ　9／00　Ｚ | |

審査請求　未請求　請求項の数１(全　５　頁)

(21)出願番号　特願平4－148328

(22)出願日　平成４年(1992)５月13日

(71)出願人　591128453
株式会社メガチップス
大阪府吹田市江坂町１丁目12番38号　江坂ソリトンビル

(72)発明者　土谷　隆
大阪府吹田市江坂町１丁目12番38号　江坂ソリトンビル　株式会社メガチップス内

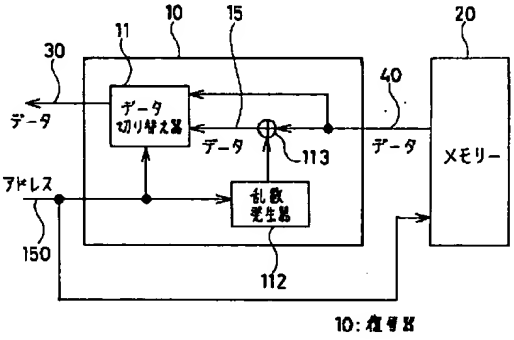
(74)代理人　弁理士　早瀬　憲一

(54)【発明の名称】　復号装置

(57)【要約】

【目的】　暗号化されたデータを復号する復号装置において、データのアクセス速度と秘匿性を両立できる装置を得る。

【構成】　暗号化されたデータとされていないデータとが混在するメモリー２０からデータを読み、そのアドレスに応じて暗号化されていないデータと、暗号化データの復号データ１５とを選択して外部に出力するデータ切り替え器１１を設けたので、メモリー２０に暗号化されたデータとされていないデータとが混在し、解読が困難になり、暗号化されていないデータは高速にアクセスできる。




10：復号装置

1

【特許請求の範囲】

【請求項1】　暗号化されたデータと暗号化されていない元のデータを混在して記憶している記憶手段から読み出したデータのうち暗号化されたデータを復号するための復号手段と、

前記記憶手段中のどのデータが暗号化されているか否かを示す識別信号に従って、前記復号手段により復号されたデータあるいは前記記憶手段中の暗号化されていない元のデータを切り替えて出力するデータ切り替え手段とを備えたことを特徴とする復号装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、暗号化されたデータの復号化を行なう復号装置に関し、特に、暗号化されたデータと暗号化されていないデータとが混在する記憶装置からデータを読出し、必要なアクセススピードに応じて出力データの切り換えを行なう装置に関するものである。

【0002】

【従来の技術】図3は従来のこの種の復号装置の構成を示す。図3において、120は暗号化されたデータを記憶するメモリー、150はこのメモリー120のアドレスデータ、110はこのメモリー120に記憶された、暗号化されたデータを復号化する復号器、112は上記アドレスデータ150に応じて乱数を発生する乱数発生器、113は上記乱数発生器112からの乱数と上記メモリー120からの暗号化されたデータ140とを加算し、元のデータ130を復元する加算器であり、上記復号器110には上記乱数発生器112と上記加算器113とが内蔵されている。

【0003】次に動作について説明する。図示しないアドレス発生器により発生されたアドレス150がメモリー120に供給されると、メモリー120からはアドレス150の値に応じた、暗号化されたデータ140が順次読み出されて、復号器110に入力される。

【0004】このアドレス150は復号器110内の乱数発生器112にも供給されており、乱数発生器112はそのアドレスの値に応じた乱数系列を順次発生する。そしてこの乱数データと上記暗号化されたデータとは加算器113にてその和を求めることにより復号され、元のデータ130となって復号器110の外部に出力される。

【0005】

【発明が解決しようとする課題】従来の復号装置は以上のように構成されており、メモリー120のデータはその内容が不当に読み出されないように、データを暗号化してメモリー120に入れている。従って、このデータを元のデータに戻すときには、乱数発生器112による乱数系列の発生、および暗号化データとの加算をしなければならない。このため、アドレス150を入れてから

2

元のデータ30が出てくるまでの時間、即ちアクセスタイムがメモリー120自身のアクセスタイムより長くなってしまう。

【0006】ところで、メモリー120中のデータによってはこのアクセスタイムが長くなっては困る場合がある。それは、読出しタイミングがクリティカルなデータであり、例えば、アドレス150を入力した場合にメモリー120自身のアクセスタイムに等しい時間でデータ130を出力して欲しいような場合である。

【0007】しかしながら、従来装置の構成では、上述のように、復号器110中の乱数発生器112によって復号のための乱数系列を発生し、これを暗号化されたデータと加え合わして復号しなければならず、この時間によってアクセスタイムが長くなってしまうという問題があった。

【0008】この発明は、上記のような従来のものの問題点に鑑みてなされたもので、メモリーのすべての元の内容を不当に解読されることなく、アクセスタイムが長くなることを防止できる復号装置を得ることを目的とする。

【0009】

【課題を解決するための手段】この発明に係る復号装置は、メモリー中にアドレスによって暗号化したデータと、していないデータを混在して入れておき、アドレスに応じて、乱数系列を加えたデータと暗号化していないデータのいずれを出力すべきかを切り替えるデータ切り替え器を設けるようにしたものである。

【0010】

【作用】この発明においては、上述のように装置を構成することによって、メモリー本来のアクセスタイムでの読出しが必要なデータに関してはこれを暗号化せずにメモリーに記憶させておき、その他のデータについてはこれを暗号化したものをメモリーに記憶させることにより、その全ての元の内容が不当に解読されることはない。

【0011】

【実施例】以下、この発明の一実施例を図について説明する。図1は本発明の一実施例による復号装置を示すブロック図である。

【0012】図において、20はメモリーであり、アドレス毎にここに記さない方法で暗号化されたデータと、暗号化されていない元のデータが混在して記憶されている。10はこの暗号化されたデータを元のデータに復元する機能を持っている復号器である。112はメモリー20に与えられるアドレス50を初期値として乱数系列を発生する乱数発生器である。113はこの乱数発生器112により発生した乱数系列とメモリー20より読み出されたデータ40のうち暗号化されたものとを加算し、復号化されたデータ15を出力する加算器、11はデータ40のうち暗号化されたものを復号化されたデー

タ１５とメモリー２０より出力されたデータ４０のうちの暗号化されていないデータとをアドレス５０に従って切替えるデータ切り替え器であり、どのアドレスの時にデータ４０のうちの暗号化されていないものかあるいはデータ１５を出力するかを記憶している。そして、上記復号器１０は乱数発生器１１２と加算器１１３とデータ切り替え器１１とで構成されている。

【００１３】次に動作について説明する。まず、メモリー２０に記憶されたデータ４０のうちそれが暗号化されて記憶されているものを読み出すときについて説明する。メモリー２０において、復号したいデータのアドレス５０を復号器１０とメモリー２０に入力する。このとき、復号器１０はメモリー２０に記憶されたデータ４０のうち、暗号化されているデータをよむ。このデータは、加算器１１３において、乱数発生器１１２からの乱数系列と加え合わされ、復号されたデータ１５となる。データ切り替え器１１は、この復号されたデータ１５を選択し、元のデータ３０として復号器１０の外部に出力する。

【００１４】このように、メモリー２０に暗号化されたデータが入っているときには、それを復号するために乱数を発生し、さらにデータの足し算をする必要がある。従って、アドレス１５０が入ってからデータ３０が出てくるまでの時間、即ちアクセスタイムはメモリー２０のアクセスタイムより大きくなってしまう。

【００１５】このメモリー２０のすべてのデータはそれを不当に読み出しコピーされないようにデータを暗号化してメモリー２０に記憶しておきたいが、あるアドレスについてはアクセスタイムが長くなっては困る場合がある。

【００１６】このようなときには、メモリー２０に暗号化したデータと、暗号化していないデータを混在しておき、アクセスタイムが長くなって困るときには暗号化されていないデータが読み出されるようにしておく。そして、データ切り替え器１１を設け、これによって、アクセスタイムが長くなって困るデータと、そうではなくむしろデータを暗号化して不当に読み出されることを防止したいデータを選択することにより、これらを混在してメモリー２０に記憶することができる。即ち、メモリー２０から不当に元のデータを読み出すことを防止でき、なおかつアクセスタイムが長くなっては困るデータについてはこれを所要のアクセスタイムで読み出すことができる。

【００１７】次に、この、暗号化されないでメモリー２０に記憶されているものを読み出すときについて説明する。メモリー２０において、復号したいデータのアドレス５０を復号器１０とメモリー２０に入力する。このとき、復号器１０はメモリー２０に記憶されたデータ４０のうち、暗号化されていないデータをよむ。

【００１８】データ４０が暗号化されていないもののときには、データ切り替え器１１はデータ４０そのものを選択し、これが元のデータ３０として復号器１０の外部に出力される。



【００１９】この選択はデータ切り替え器１１がアドレス５０を読み、そのアドレス値によってどちらを出力すべきかを決めることにより行なわれており、データ切り替え器１１にはメモリー２０の暗号化されたデータのアドレスと、暗号化されていないアドレスの情報が記憶されている。

【００２０】このように、上記実施例によれば、メモリーに、暗号化されたデータと暗号化されていないデータとを混在して記憶しておき、そのアドレスを記憶しているデータ切り替え器により、暗号化されたデータについてはこれを復号化したものを選択し、暗号化されていないものについてはこれをそのまま外部に出力するようデータを選択しこれを出力するようにしたので、データの読み出しにあたって読出し速度を優先するデータについてはこれを元データのままメモリに記憶し、読出し速度についてはこれを問わないデータについてはその秘匿性を優先して暗号化したものをメモリーに記憶することにより、不当なデータの解読防止と読み出し速度とを両立できる復号装置が得られる効果がある。

【００２１】また、上記実施例の効果については次のような説明も可能である。即ち、上記実施例装置のメモリー２０には上述のように、暗号化されたデータと、暗号化されていないデータが混在して記憶されており、どのアドレスのデータが暗号化されているが、されてないかが第三者には分からないので、メモリー２０をそのまま読み出して不当にコピーしても、内容のすべてを解読することはできない。従って、メモリー２０は復号器１０を使わないと元のデータに復元できず、このため、この復号器１０の不正使用を防止することにより、メモリーに記憶されたデータの安全性を確保することができる。

【００２２】また、上記実施例装置はデータ切り替え器１１を備えているために、アクセスタイムが復号処理のために長くなって困る場合には、暗号化していないデータをメモリー２０に記憶しておき、このデータを読み出すことによって復号処理しないで出力できる。

【００２３】なお、上記実施例では、データ切り替え器１１がメモリー２０の暗号化されたデータのアドレスと、暗号化されていないアドレスの情報を記憶することにより、切り替え動作を行なうようにしたものを示したが、図２に示す、本発明の他の実施例のように、復号器１００中にアドレスデコーダ２２を設け、データ切り替え器２１がそのデコード結果に応じてデータ１５と４０を切り替えるようにしてもよく、上記実施例と同様の効果を奏する。なお、この場合データ切り替え器２１はメモリー２０の暗号化されたデータのアドレスと、暗号化されていないアドレスの情報を記憶する必要はなく、その回路規模を縮小できることは言うまでもない。

5

【0024】また、上記各実施例では、暗号化されたデータはアドレスによって暗号化したものであったが、他のデータに基づいて暗号化してもよく、上記実施例と同様の効果を奏する。但し、この場合、乱数発生器への入力を別途用意する必要がある。

【0025】

【発明の効果】以上のように、この発明に係る復号装置によれば、暗号化されたデータと暗号化されていない元のデータを混在して記憶している記憶手段から読み出したデータのうち暗号化されたデータを復号するための復号手段と、前記記憶手段中のどのデータが暗号化されているか否かを示す識別信号に従って、前記復号手段により復号されたデータあるいは前記記憶手段中の暗号化されていない元のデータを切り替えて出力するデータ切り替え手段とを設けるようにしたので、アクセスタイムを優先するデータについてはこれを元のデータのまま記憶手段に記憶し、アクセスタイムを優先しないデータについてはこれを暗号化して記憶手段に記憶することができ、データの読出し速度と秘匿性を両立できる復号装置が得られる効果がある。

【図面の簡単な説明】

6

【図1】この発明の一実施例による復号装置のブロック図である。

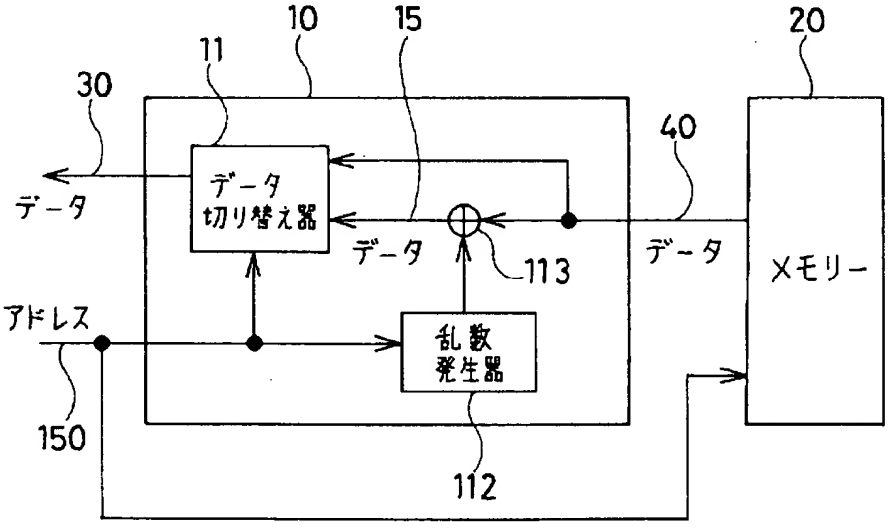
【図2】この発明の他の実施例による復号装置のブロック図である。

【図3】従来の復号装置のブロック図である。

【符号の説明】

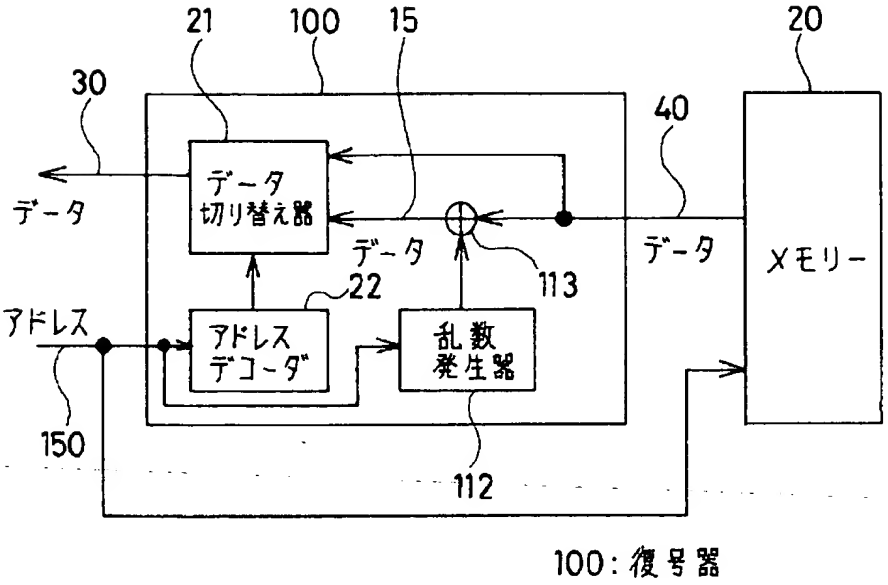
| | |
|---|---|
| 10 | 復号器 |
| 11 | データ切り替え器 |
| 21 | データ切り替え器 |
| 22 | アドレスデコーダー |
| 112 | 乱数発生器 |
| 15 | データ |
| 20 | メモリー |
| 30 | データ |
| 40 | データ |
| 100 | 復号器 |
| 110 | 復号器 |
| 120 | メモリー |
| 130 | データ |
| 140 | データ |
| 150 | アドレス |

【図1】



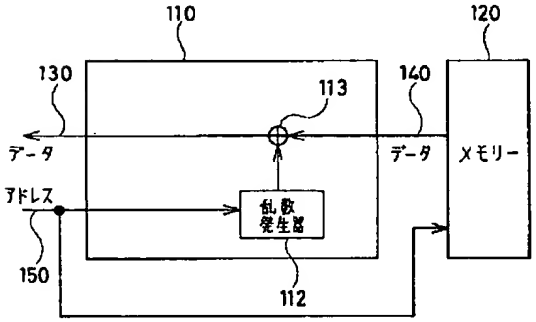

10：復号器

【図2】


21
100
15
20
30
40
データ
切り替え器
データ
データ
メモリー
113
22
アドレス
アドレス
デコーダ
乱数
発生器
150
112

100：復号器

【図3】


110
120
130
140
113
データ
データ
メモリー
アドレス
乱数
発生器
150
112